PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-234261
(43)Date of publication of application : 27.08.1999

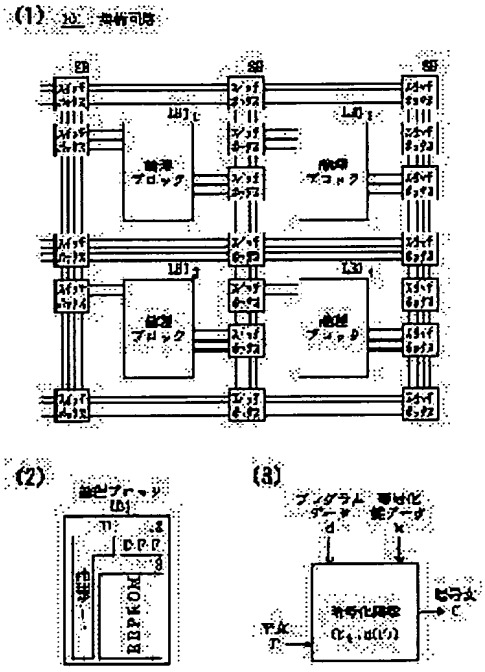
(51)Int.Cl. H04L 9/10
H01L 27/04
H01L 21/822
H04L 9/14

(21)Application number : 10-048853
(22)Date of filing : 13.02.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : FUJII KOJI

(54) INTEGRATED CIRCUIT

(57)Abstract:
PROBLEM TO BE SOLVED: To attain dispersion of elements to be analyzed by storing program data for realizing an enciphering function and enciphered key data in a memory inside a programmable logical gate.
SOLUTION: Program data (d) for characterizing an enciphering circuit and enciphering key data (k) are stored on a non-volatile memory (EEPROM) 13 arranged in a programmable logical gate in an integrated circuit 101. That is, an enciphering function is composed of a programmable logical gate that takes a logical block LB 1 as an element, and a parameter for characterizing the enciphering function is made to be the enciphering key data (k) and the program data (d) and increases more than a conventional parameter. Moreover, each parameter of the enciphering key data (k) and the program data (d) is physically stored on one EEPROM 13 on hardware, both parameters of the enciphering key data (k) and the program data D are made difficult for the third party to discriminate.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－234261

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ
Ｈ０１Ｌ　27/04		Ｈ０１Ｌ　27/04	Ｆ
21/822		Ｈ０４Ｌ　9/00	６４１
Ｈ０４Ｌ　9/14			

審査請求　未請求　請求項の数５　ＦＤ　（全７頁）

(21)出願番号　特願平10－48853

(22)出願日　平成10年(1998)２月13日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　藤井　孝治
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　川久保　新一

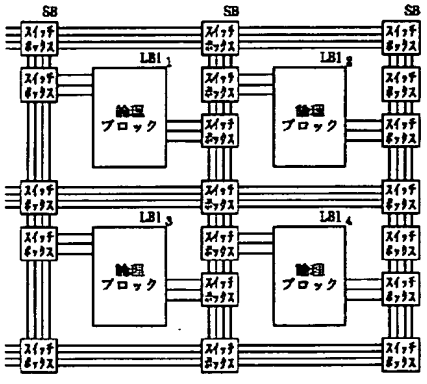
(54)【発明の名称】　集積回路

(57)【要約】

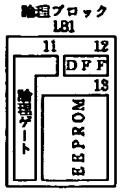
【課題】　動作解析の起点を暗号化鍵データに集中させずに、解析される要素を分散させることができる集積回路を提供することを目的とするものである。

【解決手段】　プログラマブル論理ゲートを用いて、暗号化回路、復号化回路を構成するものであり、プログラマブル論理ゲートのプログラム用記憶回路に、暗号化回路、復号化回路を実現するプログラムデータと、暗号化鍵データとの両者を格納するものである。

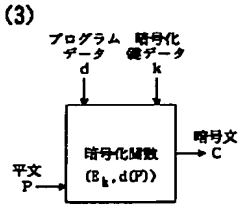
(1) 101：集積回路



(2)



(3)



E4341

1

【特許請求の範囲】

【請求項１】　暗号化関数を実現するプログラムデータと暗号化鍵データとが、１つのプログラマブル論理ゲート内のメモリに格納されていることを特徴とする集積回路。

【請求項２】　復号化関数を実現するプログラムデータと復号化鍵データとが、１つのプログラマブル論理ゲート内のメモリに格納されていることを特徴とする集積回路。

【請求項３】　暗号化関数を実現するプログラムデータと暗号化鍵データと復号化関数を実現するプログラムデータと復号化鍵データとが、１つのプログラマブル論理ゲート内のメモリに格納されていることを特徴とする集積回路。

【請求項４】　請求項１～請求項３のいずれか１項において、

上記プログラマブル論理ゲートの機能を同一に維持したまま、上記プログラムデータを変更するプログラムデータ変更手段と；上記プログラムデータ変更手段を、上記プログラマブル論理ゲート自身が繰り返して起動する変更起動手段と；を有することを特徴とする集積回路。

【請求項５】　請求項１～請求項３のいずれか１項において、

上記プログラマブル論理ゲートの機能を同一に維持したまま、上記プログラムデータを変更するとともに、上記プログラマブル論理ゲートの外部の信号に応じて、上記プログラムデータの変更動作を起動するプログラムデータ変更手段を有することを特徴とする集積回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、秘密情報を扱う集積回路において、不正者による動作解読を防止する集積回路に関するものである。

【０００２】

【従来の技術】市販ＩＣでは、多くのユーザの利益に供するために、その内部動作を公開する必要がある。一方、身分証明、電子マネー等に使用されるＩＣでは、秘密情報の漏洩を防止するために、その内部動作を隠匿する必要がある。

【０００３】図５は、従来の集積回路１００の説明図である。

【０００４】秘密情報を取り扱う従来の集積回路では、図５（１）に示すように、通常の汎用プロセッサにおける処理方式と同様の方式を採用している場合が多く、セキュリティの保持を、暗号化鍵データと復号化鍵データとの守秘性に頼っている。

【０００５】この場合、市販されているデバッグ用ツールを用いれば、様々な命令をプロセッサに実行させることが可能であり、このようにすることによって、暗号化鍵データ、復号化鍵データを読み出すこともできる。

2

【０００６】

【発明が解決しようとする課題】従来例における汎用プロセッサでは、ハードウェアが個別にモジュール化されているので、各モジュールの入出力端子から信号を取り出し、この取り出した信号を解析することによって、暗号化鍵データを傍受することが可能であり、暗号データの生成の仕組みを傍受することが可能である。観念的には、暗号化関数は、暗号化鍵データｋによって一意に決まり、平文をＰ、暗号文をＣとすると、

$C = E_k\ (P)$

である。しかし、実装形態としては、図５（２）に示すように、むしろ暗号化鍵データｋを陽に含む関数

Ｃ＝Ｅ（ｋ，Ｐ）

である。したがって、従来例においては、入力である暗号化鍵データｋ、平文Ｐと、出力である暗号文Ｃとの対応を傍受できれば、暗号解読の大きなヒントになる。

【０００７】上記のように、従来の集積回路１００においては、汎用プロセッサの動作に関して多少の知識を有していれば、電子マネー等に利用される集積回路の内部動作を解析することができる。したがって、上記従来例においては、入金データ等を不正に変更することが容易であるという問題がある。

【０００８】本発明は、動作解析の起点を暗号化鍵データに集中させずに、解析される要素を分散させることができる集積回路を提供することを目的とするものである。

【０００９】

【課題を解決するための手段】本発明は、プログラマブル論理ゲートを用いて、暗号化回路、復号化回路を構成するものであり、プログラマブル論理ゲートのプログラム用記憶回路に、暗号化回路、復号化回路を実現するプログラムデータと、暗号化鍵データとの両者を格納するものである。

【００１０】さらに、本発明は、集積回路の内部動作の解析をより困難にするために、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータの変更を行うものであり、これらの変更を、集積回路の内部信号、または、集積回路外部からの信号入力を契機として、上記変更を行うものである。

【００１１】

【発明の実施の形態および実施例】図１は、本発明の第１の実施例である集積回路１０１を示す図である。

【００１２】集積回路１０１は、プログラマブル論理ゲートを使用して構成された暗号化回路の一例である。このプログラマブル論理ゲートは、４つの論理ブロック$LB1_1$、$LB1_2$、$LB1_3$、$LB1_4$と複数のスイッチボックスＳＢとによって構成されている。論理ブロック$LB1_1$、$LB1_2$、$LB1_3$、$LB1_4$を総称して論理ブロックＬＢ１とした場合、この論理ブロックＬＢ１は、図１（２）に示すように、論理ゲート１１と、Ｄ

ＦＦ１２と、ＥＥＰＲＯＭ１３とによって構成されている。ＥＥＰＲＯＭ１３は、暗号化関数を実現するプログラムデータと暗号化鍵データとを格納するものである。

【００１３】図１（３）は、上記実施例における暗号化関数の説明図である。集積回路１０１におけるプログラマブル論理ゲート中に配置されているＥＥＰＲＯＭ１３上に、暗号化回路を特徴づけるプログラムデータｄと暗号化鍵データｋとが、格納されている。

【００１４】また、ＥＥＰＲＯＭ１３に格納されているプログラムデータｄは、単位論理ブロックＬＢ1_1、ＬＢ1_2、ＬＢ1_3、ＬＢ1_4同士の間におけるネットワークを決定するものであり、また、単位論理ブロックＬＢ1_1～ＬＢ1_4のそれぞれが実現する論理関数を決定するものである。

【００１５】ところで、図５（１）に示すように、従来の暗号化回路は、汎用のプロセッサによって実現され、平文Ｐと暗号化鍵データｋとを入力し、所定のプログラムを実行することによって、暗号化を行うものである。この場合、汎用プロセッサでは、ハードウェアがモジュール化されているので、このモジュールの入出力端子から信号を取り出すことができ、この取り出された信号を解析することによって、暗号化鍵データを傍受することが可能であり、さらには暗号データの生成の仕組みを傍受することが可能である。観念的には、暗号化関数は、暗号化鍵データｋのみによって一意に決まる。

【００１６】ところが、上記実施例においては、暗号化関数が、論理ブロックＬＢ１を要素とするプログラマブル論理ゲートによって構成されているので、暗号化関数を特徴づけるパラメータは、暗号化鍵データｋとプログラムデータｄとの２つになり、従来例におけるパラメータよりも増加する。しかも、これら暗号化鍵データｋというパラメータと、プログラムデータｄというパラメータとは、ハードウェア上、物理的に１つの不揮発性メモリ（ＥＥＰＲＯＭ１３）上に格納されているので、暗号化鍵データｋというパラメータとプログラムデータｄというパラメータとを、第三者が識別することが困難である。

【００１７】すなわち、上記実施例において、暗号文Ｃは、暗号化鍵データｋとプログラムデータｄとの両者をパラメータとする関数によって次のように表される。

【００１８】$C=E_k, d(P)$

したがって、暗号化関数を特徴づけるパラメータが、暗号化鍵データｋとプログラムデータｄの２つになり、暗号化関数のバリエーションが増加する。このために、暗号データ生成のしくみを第三者が解析することは極めて困難である。

【００１９】すなわち、上記実施例の暗号化回路構成では、暗号化関数を実現するプログラムデータｄと暗号化鍵データｋとが、１つのプログラマブル論理ゲート内のメモリに格納され、これらデータｄ、ｋを１つのプログラマブル論理ゲートの外に出す必要がない。したがって、上記実施例においては、暗号処理を行う場合における意味ある信号が、物理的なモジュールの入出力端子に発生せず、解析の手がかりを第三者に与えにくいという利点がある。

【００２０】図２は、本発明の第２の実施例である集積回路１０２を示す図である。

【００２１】集積回路１０２は、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する実施例であり、論理ブロックＬＢ2_1、ＬＢ2_2、ＬＢ2_3、ＬＢ2_4と、複数のスイッチボックスＳＢと、プログラムデータ制御ブロックＣＢ１とを有するものである。

【００２２】論理ブロックＬＢ2_1は、論理ゲート２１と、ＤＦＦ２２と、ＥＥＰＲＯＭ２３と、制御部２４とを有する。論理ブロックＬＢ2_2、ＬＢ2_3、ＬＢ2_4のそれぞれの構成は、論理ブロックＬＢ2_1の構成と同様である。

【００２３】プログラムデータ制御ブロックＣＢ１は、論理変更手段３１と、タイマ３２とを有する。論理変更手段３１は、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更するプログラムデータ変更手段の例であり、タイマ３２は、プログラムデータ変更手段（論理変更手段３１）を、プログラマブル論理ゲート自身が繰り返して起動する変更起動手段の例である。

【００２４】図３は、集積回路１０２において、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更した場合の具体例を示す図である。

【００２５】図３（１）に示す集積回路１０$2_1$は、集積回路１０２の具体例であり、論理ブロックＬＢ2_{11}が、ＡＮＤゲートとＯＲゲートとによって構成され、論理ブロックＬＢ2_{21}が、ＡＮＤゲートとＥＸＮＯＲゲートとによって構成され、論理ブロックＬＢ2_{31}が、ＮＯＲゲートによって構成され、論理ブロックＬＢ2_{41}が、ＡＮＤゲートによって構成されている。

【００２６】ここで、プログラムデータを変更することによって、集積回路１０$2_1$を、図３（２）に示す集積回路１０$2_2$に変更する。つまり、ＡＮＤゲートとＯＲゲートとによって構成されている論理ブロックＬＢ2_{11}が、ＡＮＤゲートとＮＯＲゲートとによって構成されている論理ブロック$_{12}$に変更され、ＮＯＲゲートによって構成されている論理ブロックＬＢ2_{31}が、ＯＲゲートによって構成されている論理ブロックＬＢ2_{32}に変更され、論理ブロックＬＢ2_{21}、ＬＢ$_{41}$もそれぞれ論理ブロックＬＢ2_{22}、ＬＢ$_{42}$に変更されている。

【００２７】上記変更を実行する場合、プログラムデータ制御ブロックＣＢ１におけるタイマ３２が所定時間毎に、トリガ信号を出力し、このトリガ信号に応じて、論理変更手段３１が各論理ブロックＬＢ2_1～ＬＢ$_4$に働

きかけ、各論理ブロック$LB2_1$～LB_4に設けられているＥＥＰＲＯＭ２３に格納されているプログラムデータｄが変化し、これに応じて、論理ゲート２１が変化することよって、図３に示すような変更が実行される。

【００２８】上記のようにプログラムデータｄを変更することによって、図３に示すように、集積回路102_1の論理が集積回路102_2の論理に変更され、しかも、この集積回路102_1の論理を集積回路102_2の論理に変更する場合に、集積回路102_1におけるプログラマブル論理ゲートの機能と集積回路102_2におけるプログラマブル論理ゲートの機能とが同一に維持されている。したがって、第三者による集積回路の内部動作の解析がたとえ行われたとしても、その解析が完成されるよりも前に、集積回路の変更が行われるようにタイマ３２の周期を設定すれば、第三者による集積回路の内部動作の不正な解析が、現実的には不可能になる。

【００２９】上記実施例において、集積回路における論理の変更の契機として、タイマ３２の出力信号を使用しているが、この代わりに、カウンタによる所定クロックのカウント完了を、集積回路における論理の変更の契機としてもよい。また、集積回路１０２に入力される信号が、所定の規格外の信号である場合、この規格外の信号入力を契機として、集積回路における論理の変更を実行するようにしてもよい。このようにすることによって、第三者が内部動作の解析を目的として集積回路１０２に通常の入力信号とは異なる信号を入力すると、集積回路１０２における論理の変更が直ちに実行され、集積回路１０２の内部動作の解析がより困難になる。

【００３０】図４は、本発明の第３の実施例である集積回路１０３を示す図である。

【００３１】集積回路１０３は、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する実施例であり、集積回路１０３の外部からプログラムデータ変更信号を受け、これによって、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する実施例である。

【００３２】また、集積回路１０３は、論理ブロック$LB2_1$、$LB2_2$、$LB2_3$、$LB2_4$と、複数のスイッチボックスＳＢと、プログラムデータ制御ブロックＣＢ２とを有するものである。プログラムデータ制御ブロックＣＢ２は、集積回路１０３の外部から受けたプログラムデータ変更信号に基づいて、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する手段である。このようにすれば、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する動作を、集積回路１０３の外部から、任意に実行させることができる。

【００３３】上記実施例において、暗号化関数を実現するプログラムデータを変更する場合、プログラムデータの全部を同時に変更する必要はなく、プログラムデータの一部のみを変更するようにしてもよい。

【００３４】上記実施例は、暗号化関数を実現する集積回路の一部または全部を、記憶されているプログラムデータの変更によって再構成可能な構造とするものであり、暗号化鍵データと暗号化関数とを実現するプログラムデータの双方を機密情報にしたものである。

【００３５】上記実施例によれば、暗号化を特徴づけるプログラムデータと、これらのオペランドとなる暗号化鍵データとを、物理的に同一階層にある記憶回路に分散して格納するので、上記実施例における秘密データと覚しきデータの数が、従来例における秘密データと覚しきデータの数よりも、膨大になり、したがって、不正を働こうとする第三者が解析の起点をつかむことが極めて困難である。

【００３６】上記実施例は、暗号化回路についての例であるが、上記実施例において、暗号化回路の代わりに復号化回路を想定し、暗号化鍵データの代わりに復号化鍵データを想定するようにしてもよい。つまり、復号化関数を実現するプログラムデータと復号化鍵データとが、１つのプログラマブル論理ゲート内のメモリに格納されている集積回路を想定してもよい。

【００３７】そして、上記復号化においても、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更するプログラムデータ変更手段と、上記プログラムデータ変更手段を、プログラマブル論理ゲート自身が繰り返して起動する変更起動手段とを、集積回路が有するようにしてもよい。また、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更するとともに、プログラマブル論理ゲートの外部の信号に応じて、プログラムデータの変更動作を起動するプログラムデータ変更手段を、集積回路が有するようにしてもよい。

【００３８】この場合、復号化関数を実現する集積回路の一部または全部を、記憶されているプログラムデータの変更によって再構成可能な構造とするものであり、復号化鍵データと復号化関数とを実現するプログラムデータの双方を機密情報にしたものである。また、復号化回路を特徴づけるプログラムデータと、これらのオペランドとなる復号化鍵データとを、物理的に同一階層にある記憶回路に分散して格納するので、上記実施例における秘密データと覚しきデータの数が、従来例における秘密データと覚しきデータの数よりも、膨大になり、したがって、不正を働こうとする第三者が解析の起点をつかむことが極めて困難である。

【００３９】さらに、上記実施例において、暗号化回路とともに復号化回路を設けてもよく、この場合、暗号化鍵データとともに復号化鍵データを格納するようにしてもよい。つまり、暗号化関数を実現するプログラムデータと暗号化鍵データと復号化関数を実現するプログラムデータと復号化鍵データとが、１つのプログラマブル論

理ゲート内のメモリに格納されている集積回路を想定してもよい。

【００４０】

【発明の効果】本発明によれば、集積回路における動作解析の起点を鍵データに集中させることがなく、したがって、集積回路の内部動作を解析することが困難であるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の第１の実施例である集積回路１０１を示す図である。

【図２】本発明の第２の実施例である集積回路１０２を示す図である。

【図３】上記実施例において、同一論理機能を実現しながらプログラムデータを変更した場合の具体例を示す図である。

【図４】本発明の第３の実施例である集積回路１０３を示す図である。

【図５】従来の集積回路１００の説明図である。

【符号の説明】

１０１、１０２、１０３…集積回路、

ＬＢ１、ＬＢ２…プログラマブル論理ゲートを構成する論理ブロック、

ｄ…プログラムデータ、

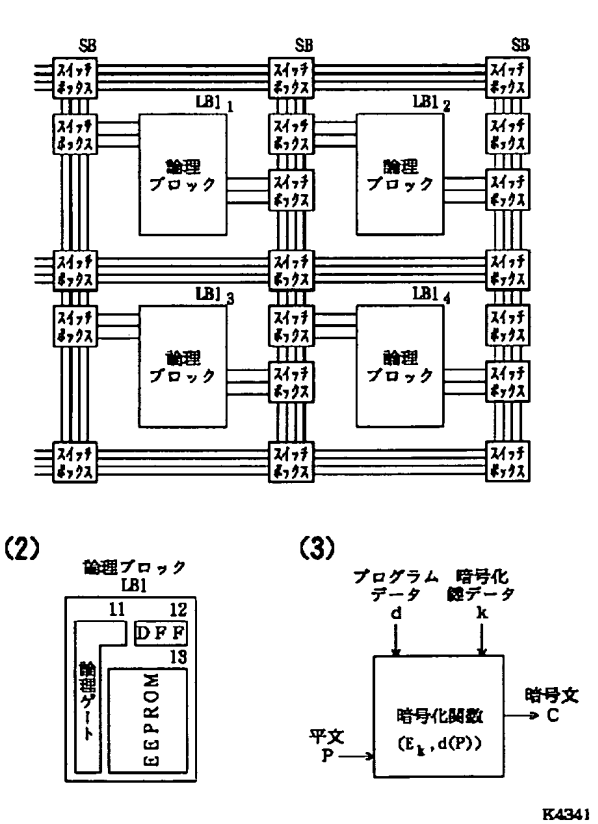
ｋ…暗号化鍵データ、

Ｐ…平文、

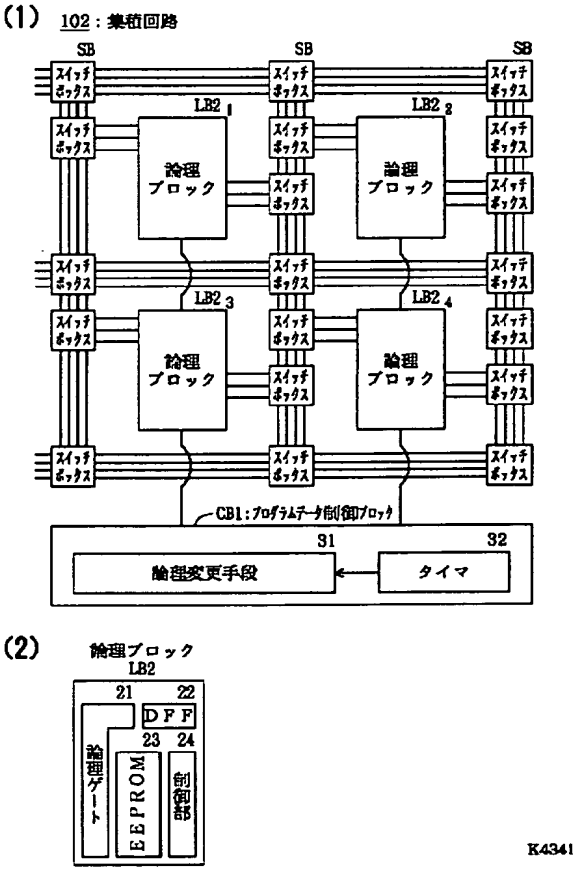
Ｃ…暗号文、

ＣＢ１、ＣＢ２…プログラムデータ制御ブロック。

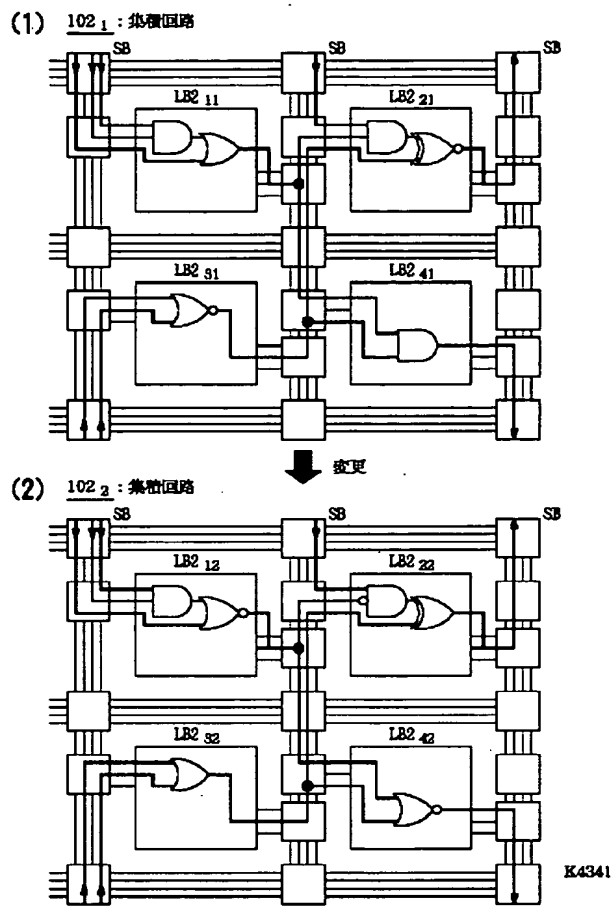
【図１】



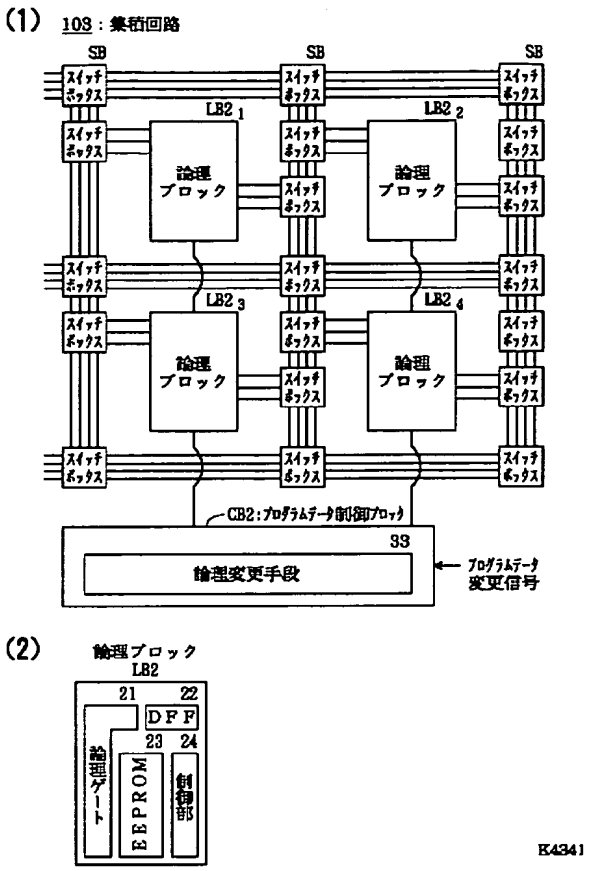
【図２】



【図３】

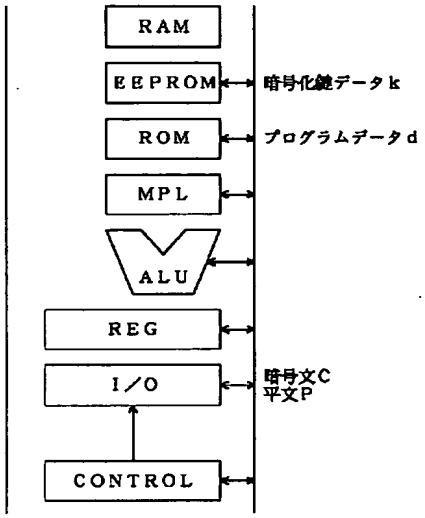

(1) 102 1 : 集積回路
SB
LB2 11
LB2 21
LB2 31
LB2 41
変更
(2) 102 2 : 集積回路
LB2 12
LB2 22
LB2 32
LB2 42
K4341

【図４】

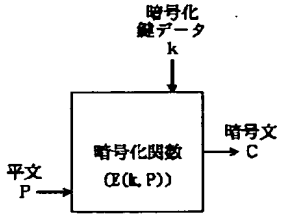

(1) 103 : 集積回路
SB
スイッチボックス
LB2 1
LB2 2
LB2 3
LB2 4
論理ブロック
CB2:プログラムデータ制御ブロック
33
論理変更手段
プログラムデータ変更信号
(2) 論理ブロック LB2
21
22
DFF
23
24
論理ゲート
EEPROM
制御部
K4341

【図５】

(1) 100：従来の集積回路



(2)



K4341